Quantum codes with bounded minimum distance

Carlos Galindo[1] , Fernando Hernando[2], Diego Ruano[3]

[1] *Universidad Jaume I, Spain, galindo@mat.uji.es*
[2] *Universidad Jaume I, Spain, carrillf@uji.es*
[3] *Aalborg University, Denmark, diego@math.aau.dk*

Polynomial time algorithms for prime factorization and discrete logarithms on quantum computers were given by Shor in 1994 [14]. Thus, if an efficient quantum computer existed (see [2, 17], for recent advances), most popular cryptographic systems could be broken and much computational work could be done much faster. Unlike classical information, quantum information cannot be cloned [5, 20], despite this fact quantum (error-correcting) codes do exist [15, 18]. The above facts explain why, in the last decades, the interest in quantum computations and, in particular, in quantum coding theory grew dramatically.

Set $q = p^r$ a positive power of a prime number p, and let $\mathbb{C}^q$ be a q-dimensional complex vector space. A $((n,K,d))_q$ quantum error correcting code is a q-ary subspace Q of $\mathbb{C}^{q^n} = \mathbb{C}^q \otimes \cdots \otimes \mathbb{C}^q$ with dimension K and minimum distance d. If $K = q^k$ we will write $[[n,k,d]]_q$.

Constructing and computing the paramters of a quantum code is in general a difficult task. In [3] Calderbank et al stablish the basis to use classical linear codes (either with the Hermitian or the Euclidean inner product) to construct a class of quantum codes named stabilizer codes. Later their results were generalized for an arbitrary finite field [13, 1]. Most of the codes known so far are obtined via the following result.

Theorem 1. *[13, 1] The following two statements hold.*

1. *Let C be a linear $[n,k,d]$ error-correcting code over $\mathbb{F}_q$ such that $C^\perp \subseteq C$. Then, there exists an $[[n,2k-n,\geq d]]_q$ stabilizer code which is pure to d. If the minimum distance of $C^\perp$ exceeds d, then the stabilizer code is pure and has minimum distance d.*

2. *Let C be a linear $[n,k,d]$ error-correcting code over $\mathbb{F}_{q^2}$ such that $C^{\perp_h} \subseteq C$. Then, there exists an $[[n,2k-n,\geq d]]_q$ stabilizer code which is pure to d. If the minimum distance $d^{\perp_h}$ of the code $C^{\perp_h}$ exceeds d, then the stabilizer code is pure and has minimum distance d.*

Codes obtained as described in Item (1) of Theorem 1 are usually referred to as obtained from the CSS construction [4, 18]. The parameters of the codes coming from Item (1) of Theorem 1 can be improved with the Hamada's generalization

[12] of the Steane's enlargement procedure [19]. Let us state the result, where wt denotes minimum weight.

Theorem 2. *[12] Let C be an $[n,k]$ linear code over the field $\mathbb{F}_q$ such that $C^\perp \subseteq C$. Assume that C can be enlarged to an $[n,k']$ linear code C', where $k' \geq k+2$. Then, there exists a stabilizer code with parameters $[[n, k+k'-n, d \geq \min\{d', \lceil \frac{q+1}{q} d" \rceil\}]]_q$, where $d' = \mathrm{wt}(C \setminus C'^\perp)$ and $d" = \mathrm{wt}(C' \setminus C'^\perp)$.*

We propose to work with the so called family of J-affine variety codes and characterize when a code within this family is contained in its dual (either Hermitian or Euclidean), see [6, 7, 8] for more details.

Consider the ring of polynomials $\mathbb{F}_q[X_1, X_2, \ldots, X_m]$ in m variables over the field $\mathbb{F}_q$ and fix m integers $N_j > 1$ such that $N_j - 1$ divides $q-1$ for $1 \leq j \leq m$. For a subset $J \subseteq \{1, 2, \ldots, m\}$, set I_J the ideal of the ring $\mathbb{F}_q[X_1, X_2, \ldots, X_m]$ generated by $X_j^{N_j} - X_j$ whenever $j \notin J$ and by $X_j^{N_j - 1} - 1$ otherwise, for $1 \leq j \leq m$. We denote by R_J the quotient ring $\mathbb{F}_q[X_1, X_2, \ldots, X_m]/I_J$.

Set $Z_J = Z(I_J) = \{P_1, P_2, \ldots, P_{n_J}\}$ the set of zeros over $\mathbb{F}_q$ of the defining ideal of R_J. Clearly, the points P_i, $1 \leq i \leq n_J$, can have 0 as a coordinate for those indices j which are not in J but this is not the case for the remaining coordinates. Denote by $\mathrm{ev}_J : R_J \to \mathbb{F}_q^{n_J}$ the evaluation map defined as $\mathrm{ev}_J(f) = (f(P_1), f(P_2), \ldots, f(P_{n_J}))$, where $n_J = \prod_{j \notin J} N_j \prod_{j \in J} (N_j - 1)$. Set $T_j = N_j - 1$ except when $j \in J$, in this last case, $T_j = N_j - 2$, consider the set

$$\mathscr{H}_J := \{0, 1, \ldots, T_1\} \times \{0, 1, \ldots, T_2\} \times \cdots \times \{0, 1, \ldots, T_m\}$$

and a nonempty subset $\Delta \subseteq \mathscr{H}_J$. Then, we define the J-affine variety code given by Δ, E_Δ^J, as the vector subspace (over $\mathbb{F}_q$) of $\mathbb{F}_q^{n_J}$ generated by the evaluation by ev_J of the set of classes in R_J corresponding to monomials $X^a := X_1^{a_1} X_1^{a_2} \cdots X_m^{a_m}$ such that $a = (a_1, a_2, \ldots, a_m) \in \Delta$. Stabilizer codes constructed from $\{1, 2, \ldots, m\}$-affine variety codes were considered in [6, 7] because they allowed us to do comparisons with some quantum BCH codes. What we call $\emptyset$-affine variety codes are simply called affine variety codes in [9]. We will stand $\mathscr{H}$ for $\mathscr{H}_\emptyset$. Notice that considering different sets J we get codes of different lengths

$$(N_1 - 1)(N_2 - 1) \cdots (N_m - 1) = n_{\{1, 2, \ldots, m\}} \leq n_J \leq n_\emptyset = N_1 N_2 \cdots N_m.$$

We provide a generalization of the bound given in [10]. We define $\varepsilon_i = 1$ if $i \in J$ and 0 otherwise.

Proposition 1. *Let $p(X) \in \mathbb{F}_q[X_1, X_2, \ldots, X_m]$ (we may also think that is a reduced class on R), with leading monomial $X^a := X_1^{a_1} X_1^{a_2} \cdots X_m^{a_m}$ where $a_i \leq T_i$ for $i = 1, \ldots, m$ then the number of points in $Z(I)$ which are not a root of $p(X)$ is:*

$$\delta_a \geq \prod_{j=1}^{m} (N_j - a_j - \varepsilon_j).$$

The minimum distance of the quantum code induced by Δ is bounded by the minimum distance of the dual $E_\Delta^\perp = E_{\Delta^\perp}$. In terms of the previous lower bound

$$d(E_{\Delta^\perp}) \geq min\{\delta_a \mid a \in \Delta^\perp\}. \tag{1}$$

Hyperbolic-like codes are constructed ad hoc in order to maximize the lower bound (1). Hyperbolic codes were studied in [11] in the particular case were $N_1 = \cdots = N_m = q^r$ and $J = \emptyset$. We propose the following generalization in this work.

Let $n_J = \prod_{i=1}^{m}(T_i + 1)$ be the length of the code (or the size of $Z(I_J)$). Fix a positive integer t, $0 \leq t \leq n_J$, define the linear code $Hyp(t,m)$, over $F_q^{n_J}$, as the image of the evaluation map of the set of monomials:

$$M_m^J(t) = \left\{ x_1^{a_1} \cdots x_m^{a_m} : 0 \leq a_i \leq T_i, 1 \leq i \leq m, \prod_{i=1}^{m} (N_i - a_i - \varepsilon_i) \geq t \right\}$$

By definition and (1) the following result is clear.

Proposition 2. *The minimum weight, d, of* $Hyp(t,m)$ *satisfies* $d \geq t$.

With this definition we maximize the dimension of a code with lower bound greater than or equal to t.

Next question is to determine its dual. We define the linear code $E(t)$, over $F_q^{n_J}$ as the image of the evaluation map of the set of monomials:

$$N_m^J(t) = \left\{ x_1^{b_1} \cdots x_m^{b_m} : \varepsilon_i \leq b_i \leq T_i, 1 \leq i \leq m, \prod_{i=1}^{m} (b_i + 1 - \varepsilon_i) < t \right\}$$

Proposition 3. *Let us assume that there exists* $j \notin J$ *such that* $p|\, N_j$. *Then* $E(t)^\perp = Hyp(t,m)$ *(where* $\perp$ *denotes the euclidean dual).*

Theorem 3. *Let* $q = p^r$ *and* $N_1 - 1, N_2 - 1 \mid q^2 - 1$ *and assume that exists* $j \notin J$ *such that* $p|\, N_j$. *If any of the following cases hold:*

(i) $J = \emptyset$ *and* $p|\, N_j$ *for all* $j \notin J$ *and exists* i *with* $N_i - 1 \mid q - 1$, *and* $N_i - 1 > t - 3$ *if* t *i odd and* $N_i - 1 > t - 4$ *if* t *is even.*

(i') $J = \emptyset$ *and exist* i *such that* $N_i - 1 \mid q - 1$ *and* $N_i - 1 \geq 2(t-2) + 1$.

(ii) $J = \{1\}$ *and* $N_2 - 1 \mid q - 1$ *and* $N_2 - 1 \geq 2(t-2) + 1$.

(iii) $J = \{1\}$ *and* $N_1 - 1 \mid q - 1$ *and* $N_1 - 1 \geq t$ *if* t *odd and* $N_1 - 1 \geq t - 1$ *if* t *even.*

(iv) $J = \{1,2\}$ *and exists* i *such that* $N_i - 1 \mid q - 1$ *and* $N_i - 1 \geq 2(t-1) + 1$.

Then there exist a quantum codes with parameters: $[[n_J, \geq n_J - 2\#E(t), \geq t]]_q$.

Theorem 4. *Let* $q = p^r$ *and* $N_1 - 1, N_2 - 1 \mid q^2 - 1$ *and assume that exists* $j \notin J$ *such that* $p \mid N_j$. *If any of the following cases hold:*

(i) $J = \emptyset$ *and* $p \mid N_j$ *for all* $j \notin J$ *and exists* i *such that* $N_i - 1 \mid q^2 - 1$ *and* $N_i - 1 > (\frac{t-1}{2} - 1)(q+1)$ *if* t *is odd and* $N_i - 1 > (\frac{t}{2} - 1)(q+1)$ *if* t *is even.*

(i') $J = \emptyset$ *and exist* i *such that* $N_i - 1 \mid q^2 - 1$ *and* $N_i - 1 > (t-2)(q+1) \geq (t-2)(q+1) + 1$.

(ii) $J = \{1\}$ *and* $N_2 - 1 \mid q^2 - 1$ *and* $N_2 - 1 > (t-2)(q+1) \geq (t-2)(q+1) + 1$.

(iii) $J = \{1\}$ *and* $N_1 - 1 \mid q^2 - 1$ *and* $N_1 - 1 > (\frac{t-1}{2})(q+1)$ *if* t *is odd and* $N_1 - 1 > (\frac{t}{2} - 1)(q+1)$ *if* t *is even.*

(iv) $J = \{1,2\}$ *and exist* i *such that* $N_i - 1 \mid q^2 - 1$ *and* $N_i - 1 > (q+1)(t-1)$.

Then there exist a quantum code with parameters $[[n_J, \geq n_J - 2\#E(t), \geq t]]_q$.

Furthermore, we present the following generalization of the Steane's enlargement procedure that allowed us to obtain excellent codes in [8].

Theorem 5. *Let* C_1 *and* $\hat{C}_1$ *be two linear codes over the field* $\mathbb{F}_q$, *with parameters* $[n, k_1, d_1]$ *and* $[n, \hat{k}_1, \hat{d}_1]$ *respectively, and such that* $C_1^\perp \subseteq \hat{C}_1$. *Consider a linear code* $D \subseteq \mathbb{F}_q^n$ *such that* $\dim D \geq 2$ *and* $(C_1 + \hat{C}_1) \cap D = \{0\}$. *Set* $C_2 = C_1 + D$ *and* $\hat{C}_2 = C_2 + D$, *that enlarge* C_1 *and* $\hat{C}_1$ *respectively, with parameters* $[n, k_2, d_2]$ *and* $[n, \hat{k}_2, \hat{d}_2]$ *(*$k_2 - k_1 = \hat{k}_2 - \hat{k}_1 = \dim D > 1$*). Set* C_3 *the code sum of the vector spaces* $C_1 + \hat{C}_1 + D$, *whose parameters we denote by* $[n, k_3, d_3]$. *Then, there exists a stabilizer code with parameters*

$$\left[\left[n, k_2 + \hat{k}_1 - n, d \geq \min\left\{d_1, \hat{d}_1, \left\lceil \frac{d_2 + \hat{d}_2 + d_3}{2} \right\rceil \right\}\right]\right]_2,$$

when $q = 2$. *Otherwise, the parameters are*

$$\left[\left[n, k_2 + \hat{k}_1 - n, d \geq \min\left\{d_1, \hat{d}_1, M\right\}\right]\right]_q,$$

where $M = \max\{d_3 + \lceil (d_2/q) \rceil, d_3 + \lceil (\hat{d}_2/q) \rceil\}$.

Acknowledgment: The authors gratefully acknowledge the support from the Spanish MINECO (Grant No. MTM2012-36917-C03-03), the Danish Council for Independent Research (Grant No. DFF-4002-00367) and from the "Program for Promoting the Enhancement of Research Universities" at Tokyo Institute of Technology.

References

[1] Aly, S.A., Klappenecker, A., Kumar, S., Sarvepalli, P.K. On quantum and classical BCH codes, *IEEE Trans. Inf. Theory* **53** (2007) 1183-1188.

[2] Bian, Z. et al. Experimental determination of Ramsey numbers, *Phys. Rev. Lett.* **111** 130505 (2013).

[3] Calderbank, A.R., Rains, E.M., Shor, P.W., Sloane, N.J.A. Quantum error correction via codes over GF(4), *IEEE Trans. Inf. Theory* **44** (1998) 1369-1387.

[4] Calderbank A.R., Shor, P. Good quantum error-correcting codes exist, *Phys. Rev. A* **54** (1996) 1098-1105.

[5] Dieks, D. Communication by EPR devices, *Phys. Rev. A* **92** (1982) 271.

[6] Galindo, C., Hernando, F. Quantum codes from affine variety codes and their subfield subcodes. To appear in *Des. Codes Crytogr.*

[7] Galindo, C., Hernando, F., Ruano, D. New quantum codes from evaluation and matrix-product codes. Preprint arXiv:1406.0650.

[8] Galindo, C., Hernando, F., Ruano, D. Stabilizer quantum codes from J-affine variety codes and a new Steane-like enlargement . Preprint arXiv:1503.00879. To appear in *Quantum Inf. Process.*

[9] Geil, O. *Evaluation codes from an affine variety code perspective*. Advances in algebraic geometry codes, Ser. Coding Theory Cryptol. 5 (2008) 153-180. World Sci. Publ., Hackensack, NJ. Eds.: E. Martinez-Moro, C. Munuera, D. Ruano.

[10] Geil, O. Roots and coefficients of multivariate polynomials over finite fields, to appear in Finite Fields and their applications.

[11] Geil, O., Høholdt, T. On hyperbolic codes, *Lect. Notes Comp. Sc.* **2227** (2001) 159-171.

[12] Hamada, M. Concatenated quantum codes constructible in polynomial time: Efficient decoding and error correction, *IEEE Trans. Inform. Theory* **54** (2008) 5689-5704.

[13] Ketkar, A., Klappenecker, A., Kumar, S., Sarvepalli, P.K. Nonbinary stabilizer codes over finite fields, *IEEE Trans. Inform. Theory* **52** (2006) 4892-4914.

[14] Shor, P.W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, in Proc. 35th ann. symp. found. comp. sc., *IEEE Comp. Soc. Press* 1994, 124-134.

[15] Shor, P.W. Scheme for reducing decoherence in quantum computer memory, *Phys. Rev. A* **52** (1995) 2493-2496.

[16] Shor, P.W., Preskill, J. Simple proof of security of the BB84 quantum key distribution protocol, *Phys. Rev. Lett.* **85** (2000) 441-444.

[17] Smith, G., Smolin, J. Putting “quantumness" to the test, *Physics* **6** 105 (2013).

[18] Steane, A.M. Simple quantum error correcting codes, *Phys. Rev. Lett.* **77** (1996) 793-797.

[19] Steane, A.M. Enlargement of Calderbank-Shor-Steane quantum codes, *IEEE Trans. Inform. Theory* **45** (1999) 2492-2495.

[20] Wootters W.K., Zurek, W.H. A single quantum cannot be cloned, *Nature* **299** (1982) 802-803.